IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 3, Issue 2, April-May, 2015
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

Data Protection: Need of Contemporary Age

Atul Kumar Pandey[1], Astitwa Bhargava[2], Sadhna[3]

[1]Assistant Professor, NLIU, Bhopal, Madhya Pradesh, India – 462044,

[2]Research Fellow, NLIU, Bhopal, Madhya Pradesh, India – 462044,

[3]M.S. in Cyber Law and Information Security, NLIU, Bhopal, Madhya Pradesh, India – 462044.

Abstract

Today data has become an indispensable part of an organization due to which protection of data has become a vital concern in this Information Age. The Information Security Compliance like PCI-DSS, ISO 27001, COBIT, etc. ensures the protection of the personal as well as the public data. This Research Paper focuses on the four dimensions of data protection, i.e., issues related to the data protection, need for protecting data, regulatory framework for data protection and the relevant Information Security Compliance required to be implemented for the protection of data.

Keywords: Data Protection, Information Technology Act 2000, Personal Data Protection Bill 2013, Information Security Compliance, PCI-DSS, ISO 27001, COBIT.

1. INTRODUCTION

The speculation about Data Protection[1] is not contemporary in it, but has turn out to be a more and more noteworthy matter in this digital epoch. In the past as jurisprudence concern data protection has gradually became ingredient of the mainstream of legal discussion as a component due to e-commerce. Data protection may perhaps be defined as a safeguard to guard the privacy, integrity[2] and security of data. The focal point of Data protection is that of individual dominion, the capacity to control. In contrast private players have seen the easiness of collecting; pooling; manipulating; and using the data (consumer's personal information[3]) turns

[1]Data Protection can be defined as legal control over access to and use of data stored in computers.
[2]As defined in ISO/IEC 27000: 2014, "Integrity means property of accuracy and completeness".
[3]Rule 2(i) of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 states, "Personal Information means any

out to be ever easier due to technical progress. E-commerce itself is conceivably the perfect medium to amass the majority of information in the most economical manner regarding consumers. It is the assertion of e-tailers and telecommunication firms that this facility to gain information[4] will help out these firms to better understanding of the consumer's requirements.

There is a maxim stated as "Knowledge is Power", now perchance it is the instance to rephrase this maxim as "Information is Profitable". As a single portion of data may be worth little, it is the skill to utilize and manipulate data to aim consumers[5] that e-commerce consider as a benefit. This tends towards an impending clash; commerce perceives information as critical for making revenue whereas, consumers are fretful about who has information with reference to them, and with what measures they collected it.

2. NEED FOR DATA PROTECTION

There are numerous grounds for splurging time, capital and effort on data protection.

- The crucial one is curtailing financial loss, trailed by compliance with regulatory requirements, upholding high-level efficiency, and conferring with client's beliefs. As computers have turn out to be more and more fundamental to business operations, data requirements have been imposed on businesses from regulator's as well as customer's end. There is a perceptible expectation that vital data is available 24X7 and either a non-functional or deficient data protection approach is not practicable.

information that relates to a natural person which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person".

[4]Section 2(1)(v) of Information Technology Act, 2000 states, "Information includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche".

[5]Section 2(d) of The Consumer Protection Act, 1986 states, "Consumer means any person who-

(i) buys any goods for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any user of such goods other then the person who buys such goods for consideration paid or promised or partly paid or partly promised, or under any person, but does not include a person who obtains such goods for resale or for any commercial purpose; or

(ii) [hires or avails of] any services for a consideration which has been paid or promised or partly paid and partly promised, or under any system of deferred payment and includes any beneficiary of such services other then the person who [hires or avails of] the services for consideration paid or promised, or partly paid and partly promised, or under any system of deferred payment."

- The solitary most significant cause to execute data protection strategies is trepidation of financial loss. Data is acknowledged as a vital corporate asset that needs to be duly cosseted. Loss of information can direct to unswerving financial losses, like lost sales, fines, or pecuniary judgments. It may also root roundabout losses from the effects of a plummet in investor assurance or customers fleeing towards the rival organization.

- One more vital business driver for data protection is the latest development in law. Governments all over the world have begun imposing new regulations on electronic communications along with stored data. Businesses face disastrous consequences for non-compliance with new regulations. Some countries clutch company executives criminally liable for non-conforming to the data protection and related laws. These regulations regularly define what information must be preserved, duration for preservation, and conditions for preservation. Other laws are framed to guarantee the privacy of the information enclosed in files, documents and databases. Loss of critical communications can be construed as violation of these regulations and may subject the organizations to pay damages and the managers to legal actions.

- A third *raison d'être,* which does not catch the consideration of the media but is significant to organizations nonetheless, is efficiency. Loss of critical data lowers the overall efficiency, as resources have to deal with protracted customer issues without the assistance of computer databases. Data loss may also end up in application failures and related system problems, making it complicated for resources to do their work. A poor data protection plan may leave resources waiting long for system restoration after a failure. During that instance, resources may be inoperative or work in reduced facility that further deteriorates the output and efficiency.

- In this digital epoch customers expect the business to operate 24X7. The downtime is not endured by customers in this global market. The inability of a business to operate because of a data loss, even a temporary one, is motivating many organizations to deploy extensive data protection

schemes. It is not only the e-commerce organizations that experience this situation. All sorts of businesses including health care, financial, manufacturing work around the clock or in any case their systems do. Even when no human resource is available, the systems are available to take and place orders, sending orders to the stockroom, and for managing financial transactions. Data protection plan should take into consideration the 24X7 expectation of customers.

3. REGULATORY FRAMEWORK FOR DATA PROTECTION IN INDIA

- **Section 43A of the Information Technology Act, 2000 (herein after IT Act):** Section 43A[6] has been added by 2008 Amendment to The Information Technology, 2000. This section fixes liability for data theft[7] or data loss[8] on those body corporate[9] that transacts among any 'sensitive personal data or information'[10] in any computer that it possesses or handles and is slipshod for implemented reasonable security practices[11] and if

[6]Section 43A of Information Technology Act, 2000 states, "Compensation for failure to protect data: Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, to the person so affected".

[7]Data theft is the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information. Data theft is increasingly a problem for individual computer users, as well as big corporate firms.

[8]Data loss is an error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing.

[9]Section 43A of Information Technology Act, 2000 explanation part clause (i) states, "Body Corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities".

[10]Rule 3 of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 states, "Sensitive Personal Data or Information of a person means such personal information which consists of information relating to:

- Passwords.
- Financial information such as Bank account or Debit Card or Credit Card or other payment instrument details.
- Physical, Physiological and Mental Health Condition.
- Sexual Orientation.
- Biometric Information.
- Medical Records and History, etc.
- Information received by Body Corporate under lawful contract or otherwise;
- User details as provided at the time of registration or thereafter; and
- Call data records.

[11]Section 43A of Information Technology Act, 2000 explanation part clause (ii) states, "Reasonable Security Practices and Procedures means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence

any person due to that incurs a 'wrongful loss or wrongful gain'[12] then, that body corporate is legally bound to pay compensation to the affected party. At the outset this section is a radically new provision as it creates a private right of action in civil law by which any person can litigate a body corporate for negligent handling of his/ her sensitive personal data or information.

- **The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011:** Ministry of Communication and Information Technology (Department of Information Technology) in exercise of its power enshrined by Section 87[13] of The Information Technology Act notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. These rules are read in juxtaposition with Section 43A that fixes liability for data theft or loss on body corporate. Rule 3 sheds light on the meaning of "Sensitive Personal Data or Information". All business houses that collect, store, receive or transact any personal data or information is compelled to implement and pursue a privacy policy to manage sensitive personal information. The privacy policy should proclaim what sort of personal information/ data is collected raison d'être for collection, disclosure norms as well as reasonable security practices[14] being adopted by that body

of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."

[12]Section 23 of The Indian Penal Code, 1860 states, "Wrongful gain is gain by unlawful means of property to which the person gaining is not legally entitled and Wrongful loss is the loss by unlawful means of property to which the person losing it is legally entitled".

[13]Section 87(1) of Information Technology Act, 2000 states "The Central Government may, by notification in the Official Gazette and in the Electronic Gazette, makes rules to carry out the provisions of this Act".

[14]Rule 8 of The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 states, "Reasonable Security Practices and Procedures.—
(1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per

corporate. These rules compels the body corporate to acquire a written consent from that person whose personal information is being collected a prior notice shall be served to that person clearly explaining purpose of information collection, intended receiver of that information. In addition to that rules obligates a body corporate to retain that collected information only for the time period essential for legitimate purpose as well as the information to be used only for that purpose for which it was collected. The person whose information is being collected shall have access to his/her collected information so that correction/ updation of on request of individual can be done. It is mandatory for the body corporate to maintain security for the collected information. It requires a body corporate to espouse a reasonable security measures together with information security policy that hems in administrative, technical and physical security controls that matches with nature of business and the information assets taken into consideration.

- **Section 72A of the Information Technology Act, 2000:** Section 72A[15] has also been added by 2008 Amendment to The Information Technology, 2000. This section states punishment for disclosure of

their documented information security programme and information security policies.
(2) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).
(3) Any industry association or an entity formed by such an association, whose members are self regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.
(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertakes significant upgradation of its process and computer resource".

[15]Section 72A of Information Technology Act, 2000 states, "Punishment for Disclosure of information in breach of lawful contract: Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees, or with both".

information in breach of lawful contract. A body corporate or intermediary is required to act as per the terms of its lawful contract and not to disclose any personal information to cause wrongful loss or wrongful gain to any other person. Disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to INR 5,00,000.

- **The Personal Data Protection Bill, 2013**

  In India we do not have a dedicated regulatory framework for data protection. So the main objective of this Bill is to provide a regulatory framework that defines data subject[16], data controller[17] and data processor[18] along with personal data, sensitive personal data and governing authorities. The terms like collect[19], store[20], process[21], disclose[22], destroy[23] that are essential steps in information lifecycle management are defined properly in this bill. This bill also describes regulation of collection, storage, processing, transfer, disclosure of personal data. This bill also describes the data protection authority and its functionalities, role and

[16]Section 2 (ic) of The Personal Data Protection Bill, 2013 states, "Data Subject means a person who is the subject of personal data".
[17]Section 2 (ia) of The Personal Data Protection Bill, 2013 states, "Data Controller means a person who, either alone or jointly or in concert with other persons, determines the purposes for which and the manner in which any personal data is processed".
[18]Section 2 (ib) of The Personal Data Protection Bill, 2013 states, "Data Processor means any person who processes any personal data on behalf of a data controller".
[19]Section 2 (g) of The Personal Data Protection Bill, 2013 states, "Collect, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a data controller obtaining, or coming into the possession or control of, any personal data of a data subject".
[20]Section 2 (y) of The Personal Data Protection Bill, 2013 states, "Store, with its grammatical variations and cognate expressions, means, in relation to personal data, to retain, in any form or manner and for any purpose or reason, any personal data".
[21]Section 2 (u) of The Personal Data Protection Bill, 2013 states, "Process, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or operation which is performed upon personal data, whether or not by automated means including, but not restricted to, organization, structuring, adaptation, modification, retrieval, consultation, use, alignment or destruction".
[22]Section 2 (l) of The Personal Data Protection Bill, 2013 states, "Disclose, with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a person who is not the data subject coming into the possession or control of that personal data".
[23]Section 2 (k) of The Personal Data Protection Bill, 2013 states, "Destroy, with its grammatical variations and cognate expressions, means, in relation to personal data, to cease the existence of, by deletion, erasure or otherwise, any personal data".

responsibilities of chairperson and members in the authority. This bill is quite clear about the punishment for offences against personal data, separate provision for offences by companies.

4. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

The Payment Card Industry Data Security Standard (herein after PCI DSS) is a set of ample requirements designed for upgrading payment account data security. It was developed by the naissance payment brands of the Payment Card Industry Security Standards Council (PCI SSC)[24], together with American Express, VISA, JCB International, Discover Financial Services and MasterCard, to facilitate the wide-ranging espousal of reliable worldwide data security measures. The standard was developed to augment control around cardholder data (CHD)[25] to trim down credit card frauds through its disclosure. Validation of compliance is carried out every twelve months, either by an external QSA (Qualified Security Assessor)[26] that produces a Report on Compliance (ROC)[27] for businesses managing huge amount of transactions, or through SAQ (Self-Assessment Questionnaire)[28] for businesses managing smaller amount of transactions. PCI DSS initially commenced as five singular programs: American Express's Data Security Operating Policy, VISA's Cardholder Information Security Program, JCB International's Data Security Program, Discover Financial Services's Information Security and Compliance and MasterCard's Site Data Protection. All corporations' (i.e. AmEx, VISA, JCB, Discover and MasterCard)

[24]The Payment Card Industry Security Standards Council (PCI SSC) is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements. The Council was founded by the five global payment brands — American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. who agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs.

[25]Cardholder Data at a minimum consists of full PAN (Permanent Account Number). It may also appear in the form of full PAN plus any of the following: cardholder name, expiration date and/or service code, sensitive authentication data.

[26]Qualified Security Assessors (QSAs) are qualified by PCI SSC to perform PCI DSS on-site assessments and they are recognized by global payment brands (i.e. American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.).

[27]Report on Compliance (ROC) is a report documenting detailed results from an entity's PCI DSS assessment.

[28]Self Assessment Questionnaire (SAQs) is a reporting tool used to document self-assessment results from an entity's PCI DSS assessment.

objectives were almost analogous "to produce an added level of shield for card issuers via guarantying that merchants meet up bare minimum levels of security when they store, process and transmit cardholder data (CHD)." This standard provides 12 requirements and 185 sub-requirements to secure Card Holder Data, the channel from where card holder data moves and the place where it is stored.

The PCI DSS standard is pertinent to any organization that processes, transmits or stores cardholder data (CHD). Either you are a merchant the PCI DSS is pertinent on you. Even if the merchant has delegated all PCI DSS doings to a third party, it is the merchant's accountability for guarantying that all the contracted parties are biddable with the standard or you are a service provider, together with a software developer, the PCI DSS is pertinent to you if you process, transmit or store cardholder data (CHD), or your actions influence the security of the cardholder data as it is being processed, transmitted or stored or you are an acquirer or a processor or an issuer the standard is pertinent to you as well as all those entities[29] that process, transmit or store cardholder data (CHD) and/or sensitive authentication data (SAD)[30].

The PCI DSS standard may apply obliquely to the entire organization or to a division of that organization if they have correctly compartmentalized the processing, transmission or storage of cardholder data away from the rest of their organization.

It is applicable to all people, processes and technologies that are concerned with the processing, transmission or storage of cardholder data. It is not only concerned with the electronic systems, but it also embraces systems including paper records like receipts, mail order forms, etc. and copy of phone conversations if they capture cardholder data being read out to call centre operators.

PCI DSS has ample requirements among which Requirement No. 3 straightforwardly says Protect Stored Cardholder Data that means if any organization is storing cardholder data

[29]Entity is used to represent any organization, corporation or business which is undergoing a PCI DSS review.

[30]Sensitive Authentication Data includes security related information (including but not limited to Card Validation Codes/ Values, full track data (from the magnetic stripe or equivalent on a chip), PINs and PIN Blocks) used to authenticate cardholders and/or authorize payment card transactions.

shall use ample number of safeguards to protect the same. All accumulated data must be encrypted. Some details should never be stored, e.g. PIN numbers and the full details on the magnetic strip. PCI DSS is a strict and as on date security standard if anything mentioned in the standard is not followed by the compliant organization that straight away moves that organization towards non-compliance to PCI DSS.

In India, the Reserve Bank of India the main regulator and supervisor of the financial systems in its year 2013 guidelines regarding "Security and Risk Mitigation Measures for Electronic Payment Transactions" clearly mentions that "*Banks should ensure that all acquiring infrastructure that is currently operational on IP (Internet Protocol) based solutions are mandatorily made to go through PCI-DSS and PA-DSS*[31] *certification. This should include acquirers, processors / aggregators and large merchants.".*[32] Since, e-commerce organizations are the IP (Internet Protocol) based Card Holder Data acquiring infrastructure so they shall be compliant with PCI-DSS.

5. ISO/ IEC 27001: 2013: INFORMATION TECHNOLOGY - SECURITY TECHNIQUES – INFORMATION SECURITY MANAGEMENT SYSTEMS - REQUIREMENTS

ISO 27001:2013 is an information security[33] standard that was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) under the joint ISO and IEC subcommittee, ISO/IEC JTC 1/SC 27. ISO 27001 is a globally renowned standard to facilitate implementation of organizational wide Information Security Management System (herein after ISMS) for the safety

[31]The Payment Application Data Security Standard (PA-DSS), formerly referred to as the Payment Application Best Practices (PABP), is the global security standard created by the Payment Card Industry Security Standards Council (PCI SSC). PA-DSS was implemented in an effort to provide the definitive data standard for software vendors that develop payment applications. The standard aims to prevent developed payment applications for third parties from storing prohibited secure data including magnetic stripe, CVV2, or PIN. In that process, the standard also dictates that software vendors develop payment applications that are compliant with the Payment Card Industry Data Security Standards (PCI DSS).

[32]For the RBI notification visit: http://rbi.org.in/scripts/NotificationUser.aspx?Id=7874&Mode=0 last visited on 1st April, 2015.

[33]Information Security means the preservation of Confidentiality, Integrity and Availability of information.

of organization's most precious information assets. ISO 27001 standards are considered like the Best Security Practices that lower down the threat of any security endangerment. Organizations which meet the standard may gain an official certification issued by an independent and accredited certification body on successful completion of a formal audit process. This standard has some requirements that may be bifurcated under P-D-C-A (Plan-Do-Check-Act) heads. Requirement number 4-7 may be taken as Plan phase in which information like context of an organization[34], needs and expectation of interested parties[35] are gathered, information security policy is established, roles and responsibilities as per the competence[36] are assigned and communicated, planning for Information Security Risk Assessment[37] and Risk Treatment[38] plans are discussed, Statement of Applicability (SOA) is created. Requirement number 8 addresses Do phase that says risk assessments should be performed in planned intervals or when there are some significant changes to the system are proposed or occur. Requirement number 9 addresses Check phase that says internal audits to check effectives[39] of ISMS; top-management[40] reviews to plan corrective actions for Non-Conformities and feedbacks on internal audits should be done on planned intervals. Requirement number 10 addresses Act phase that describes corrective actions[41] on given Non-Conformities[42] and continual improvement[43] in ISMS. It also provides 14 domains and 114 controls[44] to secure an Information Security Management System.

[34]ISO 27000: 2014 defines, "Organization means person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives".
[35]ISO 27000: 2014 defines, "Interested Party means person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity".
[36]ISO 27000: 2014 defines, "Competence means ability to apply knowledge and skills to achieve intended results".
[37]ISO 27000: 2014 defines, "Risk Assessment is overall process of risk identification, risk analysis and risk evaluation".
[38]ISO 27000: 2014 defines, "Risk Treatment means process to modify risk".
[39]ISO 27000: 2014 defines, "Effectiveness means extent to which planned activities are realized and planned results achieved".
[40]ISO 27000: 2014 defines, "Top Management means person or group of people who directs and controls an organization at the highest level".
[41]ISO 27000: 2014 defines, "Corrective Action means action to eliminate the cause of non-conformity and to prevent recurrence".
[42]ISO 27000: 2014 defines, "Non-conformity means non-fulfillment of a requirement".
[43]ISO 27000: 2014 defines, "Continual Improvement as recurring activity to enhance performance".
[44]ISO 27000: 2014 defines, "Control means measure that is modifying risk".

These 14 domains and 114 controls cover each and every facet to control and manage the ISMS of an organization from information security policy to Human Resource Security or be it access control, operations security, information security incident management or compliance with legal and contractual requirements ISO/ IEC 27001 addresses all these things.

The Central Government of India in The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011; Rule 8 stated that organizations shall consider reasonable security practices and procedures[45] and in Sub-rule 8(2) it is directly stated that organizations can implement ISO/ IEC 27001 to ensure reasonable security practices and procedures.

6. COBIT 5 FRAMEWORK: CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY: INFORMATION TECHNOLOGY (IT) MANAGEMENT AND IT GOVERNANCE

Control[46] Objectives for Information and Related Technology (herein after COBIT) is a framework created by Information Systems Audit and Control Association (ISACA) in support of information technology (herein after IT) management[47] and IT governance[48]. It is a supporting toolset that allows managers to fill up the gap between control requirements, business risks and technical issues. Major goal of COBIT is "to explore, develop, circulate and endorse a

[45]Reasonable Security Practices and Procedures means security practices and procedures designed to protect information from unauthorised access, damage, use, modification, disclosure or impairment:
- As may be specified in an agreement between the parties
- As may be specified in any law for the time being in force
- And in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

[46]Control is the means of managing risk, including policies, procedures, guidelines, practices or organizational structures which can be of an administrative, technical, management or legal nature.

[47]Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

[48]Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

trustworthy, up-to-date global set of commonly accepted information technology control objectives for daily use by business managers, assurance professionals and IT professionals". COBIT primarily an ellipsis for "Control objectives for information and related technology" (although prior to the release of the framework people had a discussion of "COBIT" like "Control Objectives for IT"), delineates a set of standard processes for the management of IT. The framework characterizes each process together with key process-activities, process inputs and outputs, performance measures, process objectives and a basic maturity model. The framework maintains IT governance by aligning and defining business goals along with IT processes and IT goals. COBIT endows with a set of suggested best practices in favor of governance with control process of information systems and technology with the quintessence of aligning IT with business.

COBIT 5 succinctly describes the importance of information and how COBIT 5 framework and its five principles and seven enablers can build an ample framework, serving organizations to attain their objectives.

COBIT 5 is a complete management and governance framework with the subsequent important features:

- A holistic approach.
- Ability to be customised to meet stakeholder's specific needs.

Securing Sensitive Personal Data/ Information is an unambiguous obligation as per the Information Technology Act, 2000 and its related Rules. As Sensitive Personal Data/ Information at present are utilized in all phases of a business, protecting it cannot be made in seclusion. Only a holistic approach, as offered by COBIT 5, can guarantee that Sensitive Personal Data/ Information is actually secured athwart the organization.

Sensitive Personal Data/ Information is exploited by a minnow for an instance, an undersized pathology laboratory, as well as giant enterprises for an instance, a transnational organization having wide e-commerce activities. The approach to safeguard Sensitive Personal Data/ Information should be customizable. COBIT 5 offers this flexibility.

COBIT 5 facilitates in identifying the following:

- Stakeholder's requirements for protecting Sensitive Personal Data/ Information, what is the subject matter to be tackled through application of COBIT 5.
- Enterprise goals to achieve the acknowledged stakeholder's needs.
- IT associated goals that will meet up the challenges of the enterprise goals.
- Enablers that will facilitate in meeting the challenges of accomplishing the IT associated goals.

The goals are summarised below:

Stakeholder's needs-Enterprise goals-IT-related goals-Enabler goals

Enablers are factors that, individually and collectively, influence whether something will work. The seven enablers of COBIT 5 will help in achieving the objective of securing Sensitive Personal Data Information. Enablers are driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve.

Enabler 1 Principles, Policies and Framework: The approach to secure Sensitive Personal Data Information is broadly based on the Organisation for Economic Co-operation and Development (OECD) principles of 'fair information practices'. Based on these principles and also on the requirements of IT Act, the 'privacy policy for SPDI (Sensitive Personal Data Information)', 'SPDI security policies' and various supporting procedures are formulated. A sound privacy framework becomes the cornerstone of securing Sensitive Personal Data Information.

Enabler 2 Processes: The IT processes themselves are derived from the stakeholder's needs. The selected processes support defining various procedures and activities, which can then be implemented for any organisation of any size, ranging from a small setup to a very large enterprise.

Enabler 3 Organizational Structures: A well-formulated organisational structure with clearly defined roles and responsibilities is necessary for securing Sensitive Personal Data Information.

Enabler 4 Culture, Ethics and Behaviour: This is as necessary for securing Sensitive Personal Data Information as are the policies and procedures. An organisation has to strongly believe in the need for doing

something right and only then it will be done.

Enabler 5 Information: Sensitive Personal Data Information is a special subset of the generic terms 'data' or 'information'. Because of Sensitive Personal Data Information's sensitive nature, it has many stringent goals for quality and security and these must be built into the various procedures for privacy and security.

Enabler 6 Services, Infrastructure and Applications: This enabler helps to create the service capabilities to meet the requirements of securing the Sensitive Personal Data Information.

Enabler 7 People, Skills and Competencies: Securing Sensitive Personal Data Information is a relatively new concept in India. It will involve sustained endeavour by organizations to internalise it and formulate it as an integral part of the business practice. This can be done by identifying and providing skills and competencies at each level in the organisation.

COBIT 5 clearly differentiates between governance and management activities and assigns roles and responsibilities accordingly. Implementation of clearly defined metrics as defined in COBIT 5 facilitates in measuring and controlling each process.

7. CONCLUSION

Data protection is a major issue in this digital epoch. In this paper we have focused on regulatory framework related to data protection in India that is being addressed by the Information Technology Act, 2000 but the major issue is that it addresses specific issues where as there are immense issues related to data protection. So there is an urgent need for a specific data protection regime in India. Organizations are required to take data protection seriously and should implement best practices to address data protection issues.

8. REFERENCES

- Lee A. Bygrave, *"Data Protection Law: Approaching its Rationale, Logic and Limits"*, 1st Edn. (Kluwer Law International, 2002), ISBN: 90-411-9870-9.
- Ed. Steve Hedley, Ed. Tanya Aplin, *"Blackstone's Statutes on IT and e-Commerce"*, 3rd Edn. (Oxford University Press, 2006), ISBN: 978-0-19-928829-8.

- Apar Gupta, *"Commentary on Information Technology Act"*, 2nd Edn. (Lexis Nexis, 2011), ISBN: 978-81-8038-702-9.
- Karnika Seth, *"Computers Internet and New Technology Laws"*, 1st Edn. (Lexis Nexis, 2013), ISBN: 978-81-8038-903-0.
- Ed. Jeremy Phillips, *"e-Commerce and IT Law Handbook"*, 2nd Edn. (Lexis Nexis, 2003), ISBN: 0-406-96342-8.
- IT Governance Frameworks and COBIT - A Literature Review http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1262&context=amcis2014.
- The effect of the Data Protection Act http://www.out-law.com/page-435.